CLAIMS

1. A method for preventing attacks in a monitored data processing system comprising the steps of:

upon detection of an intrusion, identifying a malicious code string related to the detected intrusion;

extracting the malicious code string; and

forwarding the malicious code string to an intrusion limitation subsystem to reduce further intrusions based on the malicious code string.

2. The method as claimed in claim 1, wherein the intrusion limitation subsystem comprises a pattern filter in the monitored system, and wherein said pattern filter compares incoming strings to the malicious code string for reducing further intrusions based on the malicious code string.

3. The method as claimed in claim 1, wherein the intrusion limitation subsystem comprises a response server and wherein said response server distributes the malicious code string to one or more connected systems to reduce further intrusions into such connected systems based on the malicious code string.

4. The method as claimed in claim 3, wherein the one or more connected systems comprise one or more connected monitored systems.

5. The method as claimed in claim 3, wherein the one or more connected systems comprise one or more connected monitoring systems.

6. The method as claimed in claim 1, further comprising the steps of:

monitoring system calls from a daemon executed in a memory of the monitored data processing system; and

matching the system calls with one or more of established patterns and rules contained in a pattern matcher and representing a model of normal behaviour.

7. The method as claimed in claim 6, wherein the matching of the system calls comprises establishing a non-deterministic automaton based on an analysis of executable code of the daemon.

8. The method as claimed in claim 6 further comprising the step of intercepting the system call via a subprogram of the sensor for observing the interaction of the daemon and the operating system.

9. The method as claimed in claim 8, further comprising the steps of inspecting a stack upon detection of an intrusion to retrieve an address leading to the malicious code string.

10. The method as claimed in claim 9, further comprising, on detection of an intrusion:

locating, as a first element on the stack, a return address of a system call entry code from which the subprogram departed; and

retrieving a return address of the malicious code string

pointing to a memory location in the range in which the daemon is executed from a second element on the stack positioned at or near the location of the return address of the system call entry code to facilitate finding and extracting of the malicious code string.

11. The method as claimed in claim 10, further comprising the steps of:

scanning the memory range owned by the executed daemon starting from the return address in opposite directions until on one side a first region with a plurality of similar addresses and on the other side a second region with a plurality of similar instructions that do not alter the sequential control flow is identified; and

extracting the malicious code string from between the first and second regions.

12. The method as claimed in claim 3, comprising the steps of: storing each malicious code string extracted in a database of the response server;

correlating the stored malicious code strings to find sets of malicious code strings; and

for each set, generating a signature that allows the individual identification of all malicious code strings contained in the corresponding set.

13. The method as claimed in claim 12, wherein the correlating comprises utilising an edit-distance algorithm.

14. The method as claimed in claim 13, wherein the sets have mutual edit distances smaller than a given threshold distance.

15. A computer program element comprising computer program code means which, when loaded in a processor of a data processing system, configures the processor to perform a method for preventing attacks in a monitored data processing system comprising the steps of:

upon detection of an intrusion, identifying a malicious code string related to the detected intrusion;

extracting the malicious code string; and,

forwarding the malicious code string to an intrusion limitation subsystem to reduce further intrusions based on the malicious code string.

16. Apparatus for preventing attacks in a monitored data processing system comprising:

a code extractor for identifying and extracting a malicious code string associated with a detected intrusion; and

an intrusion limitation subsystem for reducing further intrusions based on the malicious code string on receipt of the malicious code string from the code extractor.

17. The apparatus as claimed in claim 15, further comprising a sensor for monitoring system calls sent to an operating system to detect code based intrusions.

18. The apparatus as claimed in claim 15, wherein the intrusion limitation subsystem comprises: a pattern filter connected to the code extractor for receiving extracted malicious code strings and for identifying patterns within a processed data stream that match the extracted code strings to prevent further intrusions based on the malicious code strings.

19. The apparatus as claimed in claim 15, wherein the intrusion limitation subsystem comprises a response server comprising:

a database for receiving extracted malicious code strings from the code extractor;

a correlator connected to the database for assembling sets of code strings having mutual edit distances less than a given threshold distance;

a sequencer connected to the database for generating signatures, wherein a signature is generated for each set to facilitate identification of all malicious code strings contained in the corresponding set; and

a distributor connected to the database for distributing signatures to connected systems.